SOPHOS

simple + secure

Sophos Disk Encryption
Guía de herramientas

Versión: 5.61
Edición: junio de 2012

Contenido

1 Acerca de esta guía....3
2 Descarga de herramientas de cifrado....4
3 Visualización del estado del sistema con SGNState....5
4 Reversión de instalaciones fallidas con SGNRollback....6
5 Recuperación del acceso a datos cifrados con la herramienta KeyRecovery....9
6 Recuperación del sistema con la herramienta BE_Restore....12
7 Retirada de volúmenes cifrados con BEInvVol.exe....15
8 Retirada de unidades autocifrables compatibles con Opal....17
9 Soporte técnico....18
10 Aviso legal....19

1 Acerca de esta guía

En esta guía se explica cómo utilizar las herramientas de cifrado para las estaciones protegidas con el software de cifrado de Sophos.

Estas son las herramientas disponibles y tratadas en este documento:

- SGNState: visualización del estado del sistema
- SGNRollback: reversión de instalaciones fallidas
- Herramienta KeyRecovery (RecoverKeys.exe): recuperación del acceso a los equipos mediante procedimientos de desafío/respuesta
- BE_Restore.exe: reparación del sistema (registro de arranque maestro)
- BEInvVol.exe: retirada de volúmenes cifrados
- opalinvdisk.exe: retirada de unidades autocifrables compatibles con Opal

Todas las herramientas se pueden descargar en un mismo archivo .zip. La herramienta SGNState se copia también de forma automática en las estaciones durante la instalación del software de cifrado.

Público destinatario

Esta guía está dirigida a administradores de sistemas informáticos.

2 Descarga de herramientas de cifrado

1. Vaya a *http://esp.sophos.com/support/updates/*.
2. Escriba el nombre de usuario y la contraseña de su cuenta de MySophos.
3. Seleccione **Herramientas de cifrado** y extraiga el archivo ZIP en la estación.

Las herramientas estarán disponibles en la estación.

3 Visualización del estado del sistema con SGNState

La herramienta de línea de comandos SGNState muestra información sobre el estado actual (estado de cifrado e información sobre el estado más detallada) de la instalación del software de cifrado en las estaciones.

Creación de informes

SGNState también se puede utilizar como se describe a continuación:

- El código devuelto de SGNState se puede evaluar en el servidor mediante herramientas de gestión de terceros.
- SGNState /LD devuelve un resultado con formato para LANDesk que se puede pasar a un archivo.

Parámetros

Puede llamar SGNState con los siguientes parámetros:

SGNSTATE [/?] [/L] [/LD]

- El parámetro /? devuelve información de ayuda sobre los parámetros de la línea de comandos de SGNState disponibles.
- El parámetro **/L** muestra la información siguiente:

  Sistema operativo
  Versión instalada del software de cifrado
  Tipo de POA (Sophos o Opal)
  Estado de la POA (activado o desactivado)
  Estado de Wake on LAN (activado o desactivado)
  Nombre del servidor
  Modo de inicio de sesión
  Estado de activación de clientes
  Fecha (y hora) de la última replicación de datos
  Última política recibida
  Estado del cifrado (cifrado o no)

- El parámetro **/LD** devuelve esta información formateada para LANDesk.

4 Reversión de instalaciones fallidas con SGNRollback

Si se produce algún error al intentar instalar el software de cifrado en una estación, puede que no sea posible arrancar el equipo ni acceder a él para administrarlo de forma remota.

En dichos casos, puede utilizar la herramienta SGNRollback.

SGNRollback revierte de forma automática los efectos de las instalaciones fallidas del software de cifrado, lo que:

- permite arrancar el equipo bloqueado,
- elimina el software de cifrado y
- deshace todas las modificaciones efectuadas en el GINA y el resto de componentes del sistema operativo.

4.1 Usos

SGNRollback sirve para reparar instalaciones fallidas del software de cifrado en las estaciones cuando se cumple lo siguiente:

- Power-on Authentication se bloquea al iniciar el sistema por primera vez y no es posible volver a arrancar el equipo.
- El disco duro no está cifrado.

Requisitos previos adicionales

Para utilizar SGNRollback, deben cumplirse también los siguientes requisitos previos:

- SGNRollback funciona en los sistemas de recuperación WinPE y BartPE. Para utilizar SGNRollback para tareas de recuperación, intégrelo en el sistema de recuperación necesario. Consulte la documentación del sistema de recuperación correspondiente para obtener más información.

  Si SGNRollback debe autoejecutarse, el administrador que lo utilice deberá definir la configuración correspondiente en WinPE (consulte *Activación del autoinicio de SGNRollback para Windows PE* en la página 7) o BartPE (consulte *Activación del autoinicio de SGNRollback para BartPE* en la página 7).

Sistemas operativos compatibles

SGNRollback es compatible con los siguientes sistemas operativos:

- Windows XP
- Windows Vista
- Windows 7

4.2 Inicio de SGNRollback en el sistema de recuperación

SGNRollback puede iniciarse de forma manual o añadirse al inicio automático del sistema de recuperación.

4.2.1 Activación del autoinicio de SGNRollback para Windows PE

Para activar el inicio automático de SGNRollback para Windows PE, instale el kit de instalación automatizada de Microsoft Windows. En la guía del usuario del entorno de preinstalación de Windows se describe cómo crear un entorno de Windows PE y cómo iniciar aplicaciones de forma automática.

4.2.2 Activación del autoinicio de SGNRollback para BartPE

Para activar el autoinicio de SGNRollback para BartPE:

1. Cree una imagen de PE con BartPEBuilder versión 3.1.3 o posterior. Para más información, consulte la documentación de BartPE.
2. En BartPE Builder, añada la carpeta de herramientas de recuperación en el campo **Custom**.
3. Cree la imagen.
4. Copie el archivo AutoRun0Recovery.cmd en la carpeta i386 de la versión de Windows preparada para utilizarse con BartPE.
5. Cree un archivo AutoRun0Recovery.cmd que contenga las dos líneas siguientes:

   \Recovery\recovery.exe

   exit

6. Ejecute la herramienta PEBuilder desde la línea de comandos:

   Pebuilder -buildis

   Se creará una imagen ISO que incluye el archivo de autoejecución.

7. Guarde la imagen resultante en un medio de recuperación.

Al arrancar la imagen, SGNRollback se iniciará de forma automática.

4.3 Parámetros

SGNRollback puede iniciarse con el parámetro siguiente:

-drv WinDrive	Indica la letra de la unidad en la que se encuentra la instalación a reparar. Este parámetro solo puede utilizarse en modo de recuperación. Debe utilizarse en entornos de arranque múltiple para indicar la unidad correcta.

4.4 Reversión de instalaciones fallidas

1. Arranque el equipo desde el medio de recuperación que contiene el sistema de recuperación, incluido SGNRollback.

2. Inicie SGNRollback en el sistema de recuperación. Si la autoejecución está activada, SGNRollback se iniciará de forma automática. SGNRollback prepara el sistema operativo para la desinstalación del software de cifrado.
3. A continuación, deberá retirar los medios de recuperación. Después, el equipo volverá a arrancar en el modo seguro del sistema operativo.

Todas la modificaciones realizadas se eliminan y el software de cifrado se desinstala.

5 Recuperación del acceso a datos cifrados con la herramienta KeyRecovery

Para recuperar el acceso a los datos cifrados en situaciones de desastre complejas, por ejemplo, cuando Power-on Authentication se daña, puede utilizar la herramienta KeyRecovery para iniciar las estaciones a partir de un disco de recuperación mediante un procedimiento de desafío/respuesta. Para ello, el soporte de Sophos puede proporcionarle un disco de recuperación de Windows PE personalizado.

5.1 Pasos clave

Para acceder a los datos cifrados de un equipo en el que la Power-on Authentication está dañada, siga estos pasos:

1. Solicite el disco de recuperación de Windows PE personalizado para Sophos Disk Encryption al soporte de Sophos. Este disco contiene la herramienta KeyRecovery necesaria, además de los controladores del filtro del software de cifrado más recientes. Póngase en contacto con el soporte de Sophos o descárguelo en: *http://esp.sophos.com/support/knowledgebase/article/108805.html*.
2. En Sophos Enterprise Console, compruebe que se ha exportado el archivo de recuperación de claves necesario, ya que el procedimiento de desafío/respuesta lo utiliza como información de referencia. Para más información consulte el capítulo sobre cómo exportar archivos de recuperación de claves de la *Ayuda de Sophos Enterprise Console*.
3. El archivo de recuperación de claves debe estar disponible en el entorno del usuario, por ejemplo, desde una memoria USB o una ubicación de red compartida.
4. Inicie la estación desde el disco de recuperación personalizado.
5. En la estación, importe el archivo de recuperación de claves a la herramienta KeyRecovery. Inicie el desafío en la herramienta. Se generará un código de desafío.
6. En Sophos Enterprise Console, seleccione la estación correspondiente y la acción de recuperación necesaria. Después, introduzca el código de desafío generado en la estación. Se generará un código de respuesta. Para más información, consulte el capítulo Recuperación mediante el procedimiento de desafío/respuesta de la *Ayuda de Sophos Enterprise Console*.
7. En la estación, introduzca el código de respuesta en la herramienta KeyRecovery. Se descifrarán los datos cifrados.

Ahora, es posible acceder al equipo y a los datos cifrados.

5.2 Inicio de equipos desde el disco de recuperación

Compruebe que la secuencia de arranque de la configuración de la BIOS permite el arranque desde CD o DVD.

1. Inserte el disco de recuperación y reinicie el equipo. El disco se cargará de forma automática. Se abre el administrador de archivos de Windows PE. En la vista del explorador, en **PC**, puede ver la unidad y la estructura del disco.

   El contenido de la unidad cifrada no aparece en el administrador de archivos de Windows PE. El sistema de archivos, la capacidad, o el espacio libre y en uso tampoco se indican en las propiedades de la unidad cifrada.

5.3 Importación de archivos de recuperación de claves a la herramienta KeyRecovery

Compruebe que el archivo de recuperación de claves se ha exportado a una unidad accesible (por ejemplo, una unidad de memoria USB), y que la unidad se ha montado correctamente y está visible en el administrador de archivos de Windows PE del disco de recuperación.

1. En el administrador de archivos de Windows PE, seleccione la unidad en la que está almacenado el archivo de recuperación de claves. El archivo de recuperación de claves se denomina **recoverytoken.tok** y aparece en la parte derecha.
2. Seleccione **recoverytoken.tok** y arrástrelo a la unidad en la que se encuentra la herramienta KeyRecovery (**RecoverKeys.exe**). Suéltelo en el directorio **Tools\SGN-Tools**.

5.4 Inicio del desafío

1. En la parte inferior de la ficha **Inicio rápido** del administrador de archivos de Windows PE, haga clic en el icono de KeyRecovery. La herramienta KeyRecovery se inicia y muestra una lista que incluye todos los volúmenes y la información de cifrado correspondiente (identificadores de clave).
2. Seleccione la unidad que desea descifrar y haga clic en **Importar por D/R** para generar el código de desafío.

   En la página **Desafío/Respuesta**, aparecerá el código de desafío.

3. Comunique el código de desafío al centro de ayuda por teléfono o en un mensaje de texto. Si utiliza el teléfono, la **Ayuda de deletreo** puede resultar muy útil.

El centro de ayuda generará el código de respuesta en Sophos Enterprise Console. Para más información, consulte el capítulo Recuperación mediante el procedimiento de desafío/respuesta de la *Ayuda de Sophos Enterprise Console*.

5.5 Introducción del código de respuesta

El centro de ayuda deberá haber generado el código de respuesta en Sophos Enterprise Console. Para más información, consulte el capítulo Recuperación mediante el procedimiento de desafío/respuesta de la *Ayuda de Sophos Enterprise Console*.

1. En la herramienta KeyRecovery de la estación, en la página **Desafío/Respuesta**, introduzca el código de respuesta proporcionado por el centro de ayuda.
2. Haga clic en **Aceptar**. Una vez aceptado el código, la unidad seleccionada para el desafío/respuesta se descifra.
3. Para comprobar que la unidad se ha descifrado correctamente, selecciónela en el administrador de archivos de Windows PE:

   El contenido de la unidad descifrada aparece en el administrador de archivos de Windows PE. En las propiedades de la unidad descifrada, puede verse el sistema de archivos, además de la capacidad, y el espacio libre y en uso.

Se recupera el acceso a los datos almacenados en la unidad. Como resultado, es posible leer, escribir y copiar datos en y desde la unidad.

6 Recuperación del sistema con la herramienta BE_Restore

El software de cifrado cifra los archivos y las unidades de forma transparente. También es posible cifrar las unidades de arranque, por lo que es necesario que funciones como el código, los algoritmos de cifrado y las claves de cifrado estén disponibles al comenzar la fase de arranque. Si los módulos esenciales no están disponibles o no funcionan, no es posible acceder a la información cifrada.

Para solucionar daños en el sector de arranque maestro (MBR), puede utilizar la herramienta de recuperación **BE_Restore.exe**, una aplicación Win32 que debe ejecutarse en Windows, nunca en DOS.

Nota: BE_Restore.exe solo puede reparar el MBR en el disco 0. Si utiliza dos discos duros y el sistema se arranca a partir del otro, no es posible reparar el MBR.

6.1 Preparación para recuperar el sistema

Para utilizar la herramienta de recuperación BE_Restore.exe, son necesarios varios archivos adicionales. Tanto la herramienta como los archivos necesarios están incluidos en el archivo .zip descargable de herramientas de cifrado.

1. Copie todos los archivos en las carpetas KeyRecovery y Restore de las herramientas de cifrado a la memoria USB. Guárdelos todos en la misma carpeta. De lo contrario, la herramienta de recuperación no se iniciará correctamente.
2. Solicite el disco de recuperación de Windows PE personalizado para Sophos Disk Encryption al soporte de Sophos. Deberá utilizarlo para el arranque del equipo. El disco incluye los controladores de cifrado necesarios. Para obtener la imagen ISO póngase en contacto con soporte técnico o visite *http://esp.sophos.com/support/knowledgebase/article/108805.html*.
3. Grabe la imagen ISO a un disco.
4. Compruebe que la secuencia de arranque de la configuración de la BIOS permite el arranque desde CD o DVD.

6.2 Reparación del sector de arranque maestro

Para reparar un MBR dañado:

1. En el equipo afectado, conecte la memoria USB con la herramienta BE_Restore.
2. Inserte el disco de recuperación de Windows PE y reinicie el equipo. El disco se cargará de forma automática. Se abre el administrador de archivos de Windows PE.
3. Localice **BE_Restore.exe** y ejecútelo.
4. En la herramienta, abra la ficha **MBR** y seleccione **Repair MBR**.

   BE_Restore.exe localiza el kernel del software de cifrado en el disco duro, utiliza su dirección y vuelve a crear el cargador del MBR. Esto puede tardar algún tiempo.

   Nota: si se encuentra más de un kernel, se utilizará el más reciente.

Al terminar este proceso, reinicie el equipo.

6.3 Reparación del registro de arranque maestro con tabla de particiones dañada

El software de cifrado permite crear particiones principales o ampliadas nuevas, lo que provoca ciertos cambios en la tabla de particiones del disco duro correspondiente. Las tablas de particiones dañadas pueden impedir el arranque del sistema operativo después de iniciar sesión correctamente en Power-on Authentication.

Para resolver el problema:

1. En el equipo afectado, conecte la memoria USB con la herramienta BE_Restore.
2. Inserte el disco de recuperación de Windows PE y reinicie el equipo. El disco se cargará de forma automática. Se abre el administrador de archivos de Windows PE.
3. Localice **BE_Restore.exe** y ejecútelo.
4. En la herramienta, abra la ficha **MBR** y seleccione **Repair MBR**.

   Si **BE_Restore.exe** detecta alguna diferencia entre la tabla de particiones del MBR actual y la del MBR reflejado, deberá seleccionar la tabla de particiones que desee utilizar.

   Nota: el MBR reflejado es el registro de arranque maestro original de Microsoft guardado durante la configuración del software de cifrado en la estación para poder restaurarlo, por ejemplo, al desinstalar el programa. El software de cifrado actualiza la tabla de particiones del MBR reflejado si se produce algún cambio en las particiones de Windows.

5. Seleccione **From Mirrored MBR**.

   Nota: si selecciona **From Current MBR**, se utilizará la tabla de particiones del MBR actual que, en este caso, está dañada. Además de no poder arrancar el sistema, se actualizará el MBR reflejado que, por lo tanto, quedará también dañado.

6.4 Restauración de firmas de discos de Windows

Al crear por primera vez el sistema de archivos en un disco duro, Windows crea también una firma. Esta firma se guarda en el registro de arranque maestro (MBR) del disco duro en los sectores de inicio 0x01B a 0x01BB. Recuerde que, por ejemplo, las letras de unidad lógicas del disco duro dependen de la firma del disco de Windows.

Ejemplo: el administrador de Windows utiliza el administrador de discos duros de Windows para cambiar las letras de unidad lógicas de las unidades C:, D: y E: por C:, F: y Q:. Como resultado, se elimina la firma del disco de Windows en el MBR del disco duro. Tras el siguiente proceso de inicio, Windows escanea el disco duro y restaura la lista de unidades. Como resultado, las tres unidades recuperan las letras de unidad originales C:, D: y E:

Cuando este proceso tiene lugar en un equipo con el software de cifrado instalado, el controlador del filtro “BEFLT.sys” no se carga y es imposible arrancar el sistema: aparece una pantalla azul en el equipo y el error "STOP 0xED 'Unmountable Boot Volume'".

Para repararlo, es necesario restaurar la firma original del disco de Windows en el MBR del disco duro.

Este proceso se lleva a cabo también con **BE_Restore.exe.**

Nota:

Tenga cuidado al utilizar cualquier otra herramienta para reparar el MBR. Por ejemplo, los antiguos archivos FDISK.exe de MS DOS utilizados para recrear el cargador del MBR ("FDISK /MBR") pueden crear un cargador nuevo sin la firma del disco de Windows. Del mismo modo que una herramienta antigua puede eliminar la firma del disco de Windows, el cargador nuevo del MBR puede no ser compatible con los tamaños de disco duro usados de forma habitual en la actualidad. Utilice siempre versiones actualizadas de las herramientas de reparación.

7 Retirada de volúmenes cifrados con BEInvVol.exe

Para retirar volúmenes cifrados de forma segura (discos duros, memorias USB, etc.), puede utilizar la herramienta de línea de comandos **BEInvVol.exe**, basada en el estándar 5220.22-M del Departamento de Defensa de los EE. UU., que permite eliminar almacenes de claves con total seguridad. El estándar está formado por siete ciclos de sobrescritura con patrones aleatorios y alternativos.

Esta herramienta de línea de comandos está diseñada para utilizarse en equipos en los que:

- Haya instalado software de cifrado.
- Algunos volúmenes del disco duro se hayan cifrado.

La herramienta debe ejecutarse en sistemas en los que los controladores de cifrado no estén activados para evitar la retirada accidental de datos. De lo contrario, la herramienta no funcionará correctamente y aparecerá un mensaje de error.

Nota: le recomendamos que inicie el sistema desde un medio externo (por ejemplo, un disco de Windows PE) y que siga las instrucciones disponibles en la ayuda de la línea de comandos para utilizar la herramienta.

Una vez retirados, los volúmenes correspondientes dejan de ser legibles.

Según el estándar 5220.22-M, la herramienta de línea de comandos sobrescribe siete veces los sectores de arranque y las áreas de almacenamiento de claves (originales y copias de seguridad) de todos los volúmenes cifrados para purgarlos de forma permanente. No se guardan copias de seguridad de las claves aleatorias de cifrado de datos de cada volumen en la base de datos central, por lo que los volúmenes quedan perfectamente sellados.

La herramienta muestra también información sobre los volúmenes disponibles, por ejemplo, el nombre y el tamaño del volumen, e información sobre los sectores de arranque y las áreas de almacenamiento de claves. Esta información puede almacenarse en un archivo que debería guardarse en un volumen sin retirar.

Nota: una vez eliminados, no es posible recuperar los datos.

7.1 Inicio de la herramienta de línea de comandos

Sintaxis

- **xl**[**volumen**]

  Listar información sobre los volúmenes de destino. Si no se especifica el volumen de destino, listar información sobre todos los volúmenes.

- **xi**<**volumen**>

  Invalidar los volúmenes de destino si están totalmente cifrados. Con este comando, es necesario especificar el <volumen> de destino.

- <**volumen**>

  Especificar el volumen de destino = {a, b, c, ..., z, *}. <*> significa todos los volúmenes.

Opciones

- **-g0**

  Desactivar el mecanismo de registros.

- **-ga**[**archivo**]

  Modo de registro -append. Añadir entradas al final del archivo del registro de destino o crearlo si no existe.

- -**gt**[**archivo**]

  Modo de registro -truncate. Truncar el archivo del registro de destino o crearlo si no existe.

- [**archivo**]

  Especificar el archivo del registro de destino. Si no se especifica, el archivo del registro de destino predeterminado es "BEInvVol.log" en la ruta actual. No sitúe este archivo en el mismo volumen que desea invalidar.

- **-?, -h**

  Mostrar la ayuda.

Ejemplos

> **beinvvol -h**

> **beinvvol xld**

> **beinvvol xle -gac:\subdir\archivo.log**

> **beinvvol xl* -gtc:\subdir\archivo.log**

> **beinvvol xif -gt"c:\mi subdir\archivo.log"**

> **beinvvol xig -g0**

> **beinvvol xi***

8 Retirada de unidades autocifrables compatibles con Opal

Las unidades con autocifrado realizan el cifrado automático de los datos que se copian a las mismas. La organización Trusted Computing Group (TCG) ha hecho público el estándar Opal que se utiliza en este tipo de unidades.

8.1 Requisitos previos y recomendaciones

Para utilizar opalinvdisk.exe, tenga en cuenta los siguientes requisitos previos y recomendaciones:

- Antes de utilizar opalinvdisk.exe, es necesario descifrar el disco duro compatible con Opal mediante el comando **Descifrar** del menú contextual del Explorador de Windows de la estación. El comando **Descifrar** está disponible en el menú contextual cuando el cifrado se ha desactivado en la estación correspondiente desde la política.
- Son necesarios derechos de administrador.
- Es aconsejable utilizar **opalinvdisk.exe** en entornos de Windows PE.
- La herramienta **opalinvdisk.exe** inicia el servicio optativo RevertSP con el parámetro **KeepGlobalRangeKey** configurado como **Falso**. El procedimiento de retirada llevado a cabo por **RevertSP** depende de cada disco duro. Para obtener más información, consulte la sección 5.2.3 de las especificaciones TCG Storage Security Subsystem Class: Opal, versión 1.00, revisión 3.00 del estándar Opal (disponible en *www.trustedcomputinggroup.org*).

8.2 Ejecución de opalinvdisk.exe

1. Abra la línea de comandos e inicie **opalinvdisk.exe** con derechos de administrador.

   Aparecerá la herramienta e información sobre cómo utilizarla.

2. En la línea de comandos, escriba **opalinvdisk.exe <dispositivo de destino>**.

   Por ejemplo: **opalinvdisk.exe UnidadFisica0**

Si se cumplen los requisitos previos necesarios, RevertSP se inicia en la unidad especificada en <dispositivo de destino>. Si no se cumplen los requisitos previos o la unidad no es compatible con RevertSP, aparecerá un mensaje de error.

9 Soporte técnico

Para obtener asistencia técnica sobre cualquier producto de Sophos, puede:

- Visitar el fórum SophosTalk en *http://community.sophos.com/* para consultar casos similares.
- Visitar la base de conocimiento de Sophos en *http://esp.sophos.com/support/*
- Descargar la documentación correspondiente desde *http://esp.sophos.com/support/docs/*
- Enviar un email a *support@sophos.com* indicando la versión del producto de Sophos, el sistema operativo y parches aplicados, y el texto exacto de cualquier mensaje de error.

10 Aviso legal

Copyright © 1996 - 2012 Sophos Group. Todos los derechos reservados. SafeGuard es una marca registrada de Sophos Group.

Ninguna parte de esta publicación puede ser reproducida, almacenada o transmitida de ninguna forma, ni por ningún medio, sea éste electrónico, mecánico, grabación, fotocopia o cualquier otro sin la correspondiente licencia del producto, bajo dichos términos, o sin la previa autorización escrita por parte del propietario.

Sophos, Sophos Anti-Virus and SafeGuard son marcas registradas de Sophos Limited, Sophos Groupo Utimaco Safeware AG, según corresponda. Otros productos y empresas mencionados son marcas registradas de sus propietarios.

El documento Disclaimer and Copyright for 3rd Party Software, en la carpeta de instalación del producto, incluye información sobre copyright de terceros.